UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,193	04/21/2005	Alain Durand	PF030167	8417

24498 7590 05/14/2008

Joseph J. Laks
Thomson Licensing LLC
2 Independence Way, Patent Operations
PO Box 5312
PRINCETON, NJ 08543

EXAMINER	
SHEPELEV, KONSTANTIN	
ART UNIT	PAPER NUMBER
4133	

MAIL DATE	DELIVERY MODE
05/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/532,193	DURAND ET AL.	
	Examiner	Art Unit	
	KONSTANTIN SHEPELEV	4133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/21/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed on April 21, 2005 in which claims 1-4 are presented for examination.

Status of Claims

Claims 1-4 are pending; of which claim 1 is in independent form. Claims 1-4 are rejected under 35 U.S.C. 103(a).

Specification

1. The disclosure is objected to because of the following informalities: On page 9, line 20, specification includes reference to Figure 5 which appears to be a misprint since there are only three drawing provided with the application.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, and 4 are rejected under 35 U.S.C. 103(a) as being obvious over Diehl et al. (US Publication 2003/0108206 A1) in view of Menezes et al. "Handbook of Applied Cryptography, PASSAGE." Handbook of Applied Cryptography, CRC Press

Series on Discrete Mathematics and its Applications, Boca Raton, Fl, CRC Press, US, 1997, pages 497-553.

The applied reference has a common assignee and one common inventor with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). This rejection might also be overcome by showing that the reference is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

With respect to independent claim 1, Diehl discloses the limitation of "a first symmetric key for encrypting the data to be sent to a device of a second type connected to the network" (page 1, paragraph 0012) as determination of the first symmetric key.

In addition, Diehl discloses the limitation of "said first symmetric key encrypted with a second symmetric network key known only by at least one device of a second

type connected to said network" (page 1, paragraph 0013) as encryption of the first symmetric key with the aid of a second symmetric key, known to the device of the second type.

Furthermore, Diehl discloses the limitation of "encrypting the data to be transmitted with the new symmetric key" (Abstract; page 1, paragraph 0016) as encryption with the aid of the first symmetric key, of data to be transmitted.

Finally, Diehl discloses the limitation of "transmitting to a device of a second type, via said network: the data encrypted with the new symmetric key; the random number; and said first symmetric key encrypted with the second symmetric network key" (page 1, paragraph 0017) as transmission of the encrypted data and of the first encrypted symmetric key to at least one device of second type.

It is noted, however, that Diehl does not disclose the limitations of "generating a random number" and "computing a new symmetric key as a function of the first symmetric key and said random number." On the other hand, Menezes discloses abovementioned limitations (pages 552-553, Example 13.9) as C decrypts the key list to obtain Kx, computes S from R, then encrypts S under Kx and transmits it to X. S is analogously transmitted to Y, and can be recovered by both X and Y. Where, C is a Central trusted node, X and Y are terminals, Kx is a terminal key for the terminal X, S is a session key, and R is a random value. It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate teachings of Menezes into the system of Diehl because it would increase the security for the transmitted data through the use of the key-encrypting key.

With respect to claim 2, Menezes discloses the limitation of "the function used to compute the new symmetric key is a one-way derivation function" (page 498, lines 5-6) as choosing *f* to be a one-way function precludes control of the final key value by either party.

With respect to claim 4, Diehl discloses the limitation of "decrypting, with the second symmetric network key, the encryption of the first symmetric key" (Abstract; page 1, paragraph 0018) as decryption of the first symmetric key with the aid of the second symmetric key.

In addition, Diehl discloses the limitation of "decrypting the data received with the new symmetric key thus obtained" (page 1, paragraph 0018) as decryption of the encrypted data with the aid of the first symmetric key.

It is noted, however, that Diehl does not disclose the limitation of "determining, based on the first symmetric key obtained at step (e) and on said random number, the new symmetric key." On the other hand, Menezes discloses (page 553, lines 1-2) the session key derived as a function of a random number and master key. It would be obvious to one of the ordinary skill in the art that random value R can be obtained from the session key through the application of the function to the master key.

4. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Diehl et al. (US Publication 2003/0108206 A1) in view of Menezes et al. "Handbook of Applied

Cryptography, PASSAGE." Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, Fl, CRC Press, US, 1997, pages 497-553 as applied to claim 1 and in further view of Fischer (US Patent 5,475,826).

With respect to claim 3, it is noted that neither Diehl nor Menezes disclose the limitation of "the function is a hash or encryption function." On the other hand, Fischer discloses the abovementioned limitation (column 1, lines 37-39) as It is well-known that file integrity may be protected by taking a one-way hash (e.g., by using MD5 or the secure hash algorithm SHA). It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Fischer into the system of Diehl and Menezes because the use of one-way has would facilitate better protection of the encryption key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KONSTANTIN SHEPELEV whose telephone number is (571)270-5213. The examiner can normally be reached on Mon - Thu 7:30 - 17:00, Fri 7:30 - 16:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Coby can be reached on (571) 272-4017. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Konstantin Shepelev/
Examiner, Art Unit 4133

5/12/2008
/Frantz Coby/
Supervisory Patent Examiner
Art Unit 4133